CLAIMS

What is claimed is:

1. A method for booting up a computer system in a secure fashion comprising the steps of:

a) determining the presence of a security feature element during an initialization of the computer system wherein the security feature element includes a public key and a corresponding private key;

b) storing a portion of the public key in a nonvolatile memory within the computer system if the security feature element is present; and

c) utilizing an algorithm to determine the presence of the security feature element prior to a subsequent boot-up of the computer system.

2. The method of claim 1 wherein the security feature element comprises a security card.

3. The method of claim 2 wherein the security card provides for tamper detection of the computer system and the security card, temperature monitoring of the computer system and voltage status reporting of the computer system.

4. The method of claim 1 wherein step c) is performed during a Power-On-Self-Test (POST) sequence.

5. The method of claim 4 wherein step c) further comprises:

c1) determining the presence of the security card.

6. The method of claim 5 wherein step c1) further comprises:

c1a) determining if the computer system has been subjected to a tamper event if the security card is present.

7. The method of claim 6 wherein step c1) further comprises:

c1a) determining whether a security card was previously present in the computer system if the security card is not present.

8. The method of claim 7 wherein step c1) further comprises:

c1b) clearing the portion of the public key stored in the non-volatile memory of the computer system if a security card was previously present in the computer system; and

c1c) prompting for an authorization prior to booting up the computer system.

9. The method of claim 7 wherein step c1) further comprises:

c1b) booting up the computer system if the security card was not previously present in the computer system.

10. The method of claim 6 wherein step c1) further comprises:

c1b) booting up the computer system if the computer system has not been subjected to a tamper event.

11. The method of claim 6 wherein step c1) further comprises:

c1b) determining whether the security card is an added feature of the computer system, wherein the determination is based on a previous POST sequence, if the computer system has been subjected to a tamper event.

12. The method of claim 11 wherein step c1) further comprises:

c1c) clearing the portion of the public key stored in the nonvolatile memory of the computer system if the card is a newly added feature of the computer system; and

c1d) prompting for an authorization prior to booting up the computer system.

13. The method of claim 11 wherein step c1) further comprises:

c1c) comparing the public key on the security card with the portion of the public key stored in the nonvolatile memory of the computer system if the security card is not a newly added feature of the computer system.

14. The method of claim 13 wherein step c1) further comprises:

c1d) booting up the computer system if the public key on the security card matches the portion of the public key stored in the nonvolatile memory of the computer system.

15. The method of claim 13 wherein step c1) further comprises:

c1d) clearing the portion of the public key stored in the nonvolatile memory of the computer system;

c1e) clearing the public key and the corresponding private key stored on the security card; and

c1f) booting up the computer system.

16. A system for booting up a computer in a secure fashion, the system comprising:

means for determining the presence of a security feature element during an initialization of the computer system wherein the security feature element includes a public key and a corresponding private key;

means for storing a portion of the public key in a nonvolatile memory within the computer system if the security feature element is present; and

means for utilizing an algorithm to determine the presence of the security feature element prior to a subsequent boot-up of the computer system.

17. The system of claim 16 wherein the security feature element comprises a security card.

18. The system of claim 17 wherein the security card provides for tamper detection of the computer and the security card, temperature monitoring of the computer and voltage status reporting of the computer.

19. The system of claim 18 wherein the algorithm is utilized during a Power-On-Self-Test (POST) sequence.

20. The system of claim 19 wherein the means for utilizing the algorithm further comprises:

means for determining the presence of the security card.

21. The system of claim 20 wherein the means for utilizing the algorithm further comprises:

_means for determining if the computer has been subjected to a tamper event if the security card is present.

22. The system of claim 20 wherein means for utilizing the algorithm further comprises:

means for determining whether a security card was previously present in the computer if the security card is not present.

23. The system of claim 22 wherein the means for determining the presence of the security card further comprises:

means for clearing the portion of the public key stored in the non-volatile memory of the computer if a security card was previously present in the computer; and

means for prompting for an authorization prior to booting up the computer.

24. The system of claim 22 wherein the means for determining the presence of the security card further comprises:

means for booting up the security system if the security card was not previously present in the computer.

25. The system of claim 21 wherein the means for determining the presence of the security card further comprises:

means for booting up the computer if the computer has not been subjected to a tamper event.

26. The system of claim 21 wherein the means for determining the presence of the security card further comprises:

means for determining whether the card is a newly added feature of the computer, wherein the determination is based on a previous POST sequence, if the computer has been subjected to a tamper event.

27. The system of claim 26 wherein the means for determining the presence of the security card further comprises:

means for clearing the portion of the public key stored in the nonvolatile memory of the computer if the card is a newly added feature of the computer; and

means for prompting for an authorization prior to booting up the computer.

28. The system of claim 26 wherein the means for determining the presence of the security card further comprises:

means for comparing the public key on the security card with the portion of public key stored in the nonvolatile memory of the computer if the security card is not a newly added feature of the computer.

29. The system of claim 28 wherein the means for determining the presence of the security card further comprises:

means for booting up the computer system if the public key on the security card matches the portion of the public key stored in the nonvolatile memory of the computer.

30. The system of claim 28 wherein the means for determining the presence of the security card further comprises:

means for clearing the portion of the public key stored in the nonvolatile memory of the computer;

means for clearing the public key and the corresponding private key stored on the security card; and

means for prompting for an authorization prior to booting up the computer.